REMARKS

With this amendment the independent claims 1, 14 and 15 have been amended. Claims 1-8 and 14-19 are pending of which claims 1 (system), 14 (system) and 15 (method) are independent claims.

The Discussion At The Interview

The applicants thank Examiner Holloway for the interview of February 17, 2009. At the interview the Examiner agreed that "to specify [as in the proposed claims] a separate rolling access code that changes with each combined signal transmission and verifying authorization without transmitting a signal to the transmitter" appears to overcome the Hsu reference. But at the interview, the Examiner raised the issue of whether a combination of Gullman, Waraksa, and Flick rendered the claims obvious. As this was a new type of rejection, applicants attorney indicated he would address this combination with this amendment.

The Rejection Pending At The Time Of The Interview – NON FINAL

The rejections pending at the time of the interview were solely obviousness rejections.

In his last office action the Examiner asserted claims 1, 2, 5, 7-8, 14-16 and 19 are obvious in view of Hasu (6,041,410), Flick (6,140,939 and Waraksa (5,412,379).

In his last office action the Examiner asserted claims 1, 2, 5, 7-8, 14-16 and 19 are obvious in view of Hasu (6,041,410), Flick (6,140,939) and Waraksa (5,412,379) and further in view of Gullman (5,280,057).

In his last office action the Examiner asserts claims 3 and 17 are obvious in view of Hasu (6,041,410), Flick (6,140,939), Waraksa (5,412,379), Gullman (5,280,057), and further in view of Nicholls (for the teaching of an electroluminescent fingerprint sensor).

In his last office action the Examiner asserted claims 4 and 18 are obvious in view of Hasu (6,041,410), Flick (6,140,939) and Waraksa (5,412,379) and Gullman (5,280,057) and further in view of Toyoda (5,999,637 for CCDs).

Finally, in his last office action the Examiner asseted claim 6 is obvious in view of Hasu (6,041,410), Flick (6,140,939), Waraksa (5,412,379), Gullman (5,280,057), and further in view of Fitzgibbon (5,751,224).

As Generally Agreed At The Interview The Claims Distinguish Hsu

As discussed at the interview, the claims distinguish Hsu because -

1. Applicants' barrier movement operator does not require a transmitter which transmits encrypted signals.

2. Applicants' transmitter is outside a secured area does not require a receiver.

3. In applicants' device a receiver at the transmitter is not needed.

4. Applicants have an access code which constantly changes as a result of each transmission.

5. Hsu does not describe the transmission of constantly changing authorization codes (what Hsu calls CRC values). These CRC values effect access, represent the finger print and do not change. Rather they are encrypted using keys from the door where the door keys are changing with each transmission. Applicants' access code is separate from the finger print code. Applicants' rolling code which effects access is clearly described in the claims as separate and different from a finger print code or Hsu's CRC value. Applicants' access code (which effects the access to a secured area) is an always changing rolling code.

6. Hsu does not suggest a combining an always changing access code with a separate finger print code and separating the always changing authorization code and signal from the finger print code and signal as claimed. Hsu does not suggest combining separate codes, transmitting a combined code and then separating the combined code at the operator as claimed.

7. *Hsu requires a transmission from the receiver for access to send the public door key back to the transmitter.* The device and method of the claims do not and exclude such a transmission.

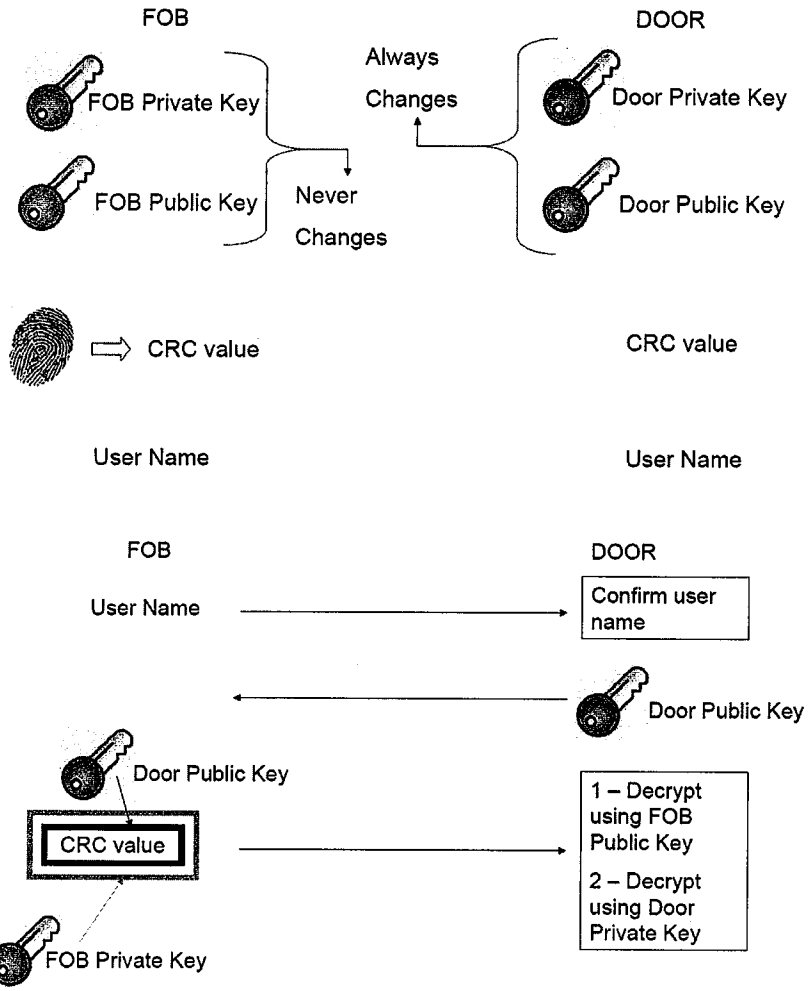
The Problem Solved By Applicants

In the past, wireless security systems were vulnerable to code grabbers which would read and store codes from a transmitter being used to gain access to a secured area. Because of that problem, rolling code which changes the access code with each use of that code to gain access to a secured area has been used to defeat code grabbing. Transmitters using rolling code, however, can be lost or stolen. This also compromises security. Transmitters or security systems which relied solely on biometric data, such as finger prints, were thought nearly invulnerable. See Declaration of Fitzgibbon attached to previous amendment. That was not true as will be explained in more detail below. The claims herein describe a barrier operator system and method which address and ***inexpensively*** solve this security problem by combining the use of rolling code which is known with finger print identification technology which is also known. **Applicants' barrier movement operator does not require a transmitter which transmits encrypted signals. Nor does applicants' transmitter which is outside a secured area require a receiver.** Rather, as described in the claims, only the transmitter transmits a changing code which authorizes movement of the barrier. **A receiver at the transmitter is not needed.** Rolling code and code representative of an authorized user's finger print are combined and transmitted as a changing authorization code without (1) double encryption and (2) without the barrier movement operator being required to transmit to the transmitter a changing door "private key." The changing combined authorization code provides inexpensive security for finger print biometric data and provides a unique combination which solves the vulnerability of both biometric and rolling code technologies to enhance security.

General Discussion Of Hsu

Hsu only involves transmissions indicating valid fingerprints using a double encryption method as described by Hsu at column 6, line 42 through column 7, line 34. In this method the fob has private and public keys and the door has private and public keys. The keys for the fob never change. Hsu at column 7, line 4. The keys for the door always change with a transmission. Hsu at column 7, lines 13-16. The finger print is sensed at the fob and the finger

print code, which Hsu calls "CRC", is read into the transmitter of the fob. Upon receipt of a user name from the fob transmitter, the door generates a random pair of public-private keys and transmits the public key to the fob and the fob receiver without encryption. Hsu column 7, line 17-19. If the fob has validated the user's ID by matching the sensed fingerprint with reference image, the fob performs two levels of encryption on the fingerprint (CRC). The first encryption is with the door's public key. Then the CRC is encrypted using the fob's private key. Then the doubly encrypted CRC is transmitted to the door where it is decrypted. The process is graphically shown below.



Examiner acknowledges that Hsu does not show a comparison of finger print at the operator. See page 2 of Office Action bottom. Hsu scans the finger print at the fob and compares: A person 12 has fingerprint scanned and compared to a reference print at fob 14. A confirming message is sent to door 12. Hsu enrolls and stores a finger print image at 32 and then a sensed finger print is compared with the referenced image using a correlator 28 at the transmitter.

Hsu does not describe the transmission of constantly changing authorization codes. The authorization codes (the CRC values) in Hsu do not change. Rather they are encrypted using keys from the door where the door keys are changing with each transmission.

Hsu's discussion ***does not suggest a combining and a separating an always changing combined authorization signal as claimed.*** Hsu does not suggest combining codes, transmitting a combined code and then separating the combined code at the operator as claimed. Hsu's authorization code never changes, but is encrypted. Applicants' authorization code always changes. Hsu's apparatus is complicated and requires a receiver and transmitter at the door. Hsu also requires a receiver at the transmitter outside the secured area. In short Hsu requires transreceivers at both the operator inside the secured area and at the finger print/reader on the fob outside the secured area. Hsu does not suggest the claims.

Hsu requires a transmission from the receiver for access to send the public door key back to the transmitter. The device and method of the claims exclude such a transmission. For example see claim 1 "separating the portion of the received changing combined authorization code signal representative of the sensed fingerprint from the separate rolling access code, and reading the stored signal representative of the sensed finger print to verify authorized users without transmitting a signal to the transmitter ." For example in method claim 15, "the finger print circuit effective for receiving a finger print identifying signal representative of the sensed finger print, separating the received combined signal representative of the sensed fingerprint from the separate rolling access code, and reading the stored signal representative of a finger print to verify authorized users without transmitting a signal to the transmitter."

Flick

Flick is only concerned with finger print identification and it is this fingerprint identification that provides the required security.

Flick scans the finger print and sends only that fingerprint data --a vehicle start controller 86 receives biometric sensor data from remote transmitter 50. There can be a comparison at the transmitter or operator, but so-what. ***There is NO teaching of transmitter 50 sending a combined code which includes both a rolling code (which represents a particular transmitter) and finger print data.***

Flick does not suggest determining whether both fingerprint and rolling code are acceptable.

Flick does not suggest transmitting an always changing authorization code which is a combination the finger print with an access code and then splitting them.

Waraksa

Waraksa describes a passive keyless entry system. Transmitter 24 generates what the Examiner calls a rolling code, but this reference does not teach the use of both rolling code and fingerprint data or whether both are acceptable.

Waraksa does not teach combining a code representative of the finger print with an access code and then recognizing the access code and fingerprint code for access to a secure area. As can be seen by reference to column 8, lines 46 to 55 and column 10, lines 37 to 55, Waraksa describes a clock for which a clock code is generated and which changes. This is not a rolling code, but this is not relevant because applicant acknowledges rolling code is known.

The references do not suggest using a changing combined authorization code which is a combination of a code representative of a fingerprint code and an ever changing rolling code.

The Claims Are Non-Obvious Over The Applied Art Of Hsu, Flick and Waraksa

None of the references alone or in combination teach or suggest a system that determines the acceptance of an ever changing authorization code which is a combination of both a user fingerprint and a rolling code. Since elements of claim 1 are not taught or suggested by the prior art, it is believed that independent claims 1, 14 and 15 are allowable for this reason.

Hsu and Flick completely rely on the use of a signal representative of finger print data for entry into a secured area. Hsu requires a double encryption of a never changing CRC authorization code representative of a finger print and requires receipt of and the transmission of signals from the door and receipt of the signal from the door by the remote transmitter. Hence, while Hsu does to some extent protect against code grabbing biometric data, it does so in a complicated and expensive way.

The Obviousness Rejection Proposed At The Interview Based Upon Gullman --- Gullman Does Not Have A Rolling Code Which Is Event Driven (As Opposed To Time Driven) And Does Not Verify A User And Then Accept A Rolling Code After Verification.

Gullman does not describe a rolling code which varies ***as a result of each transmission*** of the rolling code (see all independent claims), nor does Gullman describe ***verifying a user and then accepting a rolling code after a user has been verified with biometric data,*** e.g. a finger print (see all independent claims).

At the interview, Examiner Holloway raised the issue of in effect making Gullman his "main reference" in view of Gullman's discussion at column 5, lines 15-33. At this point in the Gullman patent, Gullman discusses encrypting the time of day from a time clock, a fixed code and a biometric code to generate an encrypted security token. Gullman describes a host system which includes a decryption module which breaks the token down into the biometric code, time varying code and the fixed code. The Examiner has equated the time varying code generated with a clock with applicants' use of a rolling code which changes as a result of each transmission according to an algorithm. The practical difference in security provided by applicants' system and Gullman differ starkly.

In Gullman's system a code grabber with a good clock can grab and break a biometric data code (which is fixed), a fixed code and then understand how the code varies with a clock. Having his own clock, the code grabber can understand the varying code (which varies with time). This is not the case with the apparatus and method of the claims. In applicants' claims, the varying code is even driven, not time driven. Hence the an algorithm changes as a result of the transmissions. This makes the code difficult to grab and understand what the next transmission should be.

There also is a second major difference between the claims and Gullman. Gullman uses biometric data as a "payload" to obtain access to a secured area. It as if the biometric data is just another fixed code for access. In applicants' system, a user is verified with a fixed code, ***then*** access is achieved with the acceptance of the rolling code. It is this sequence that makes the rolling code movable barrier of the claims so difficult to grab and use. The biometric data further secures a portable remote transmitter from theft and later use. The thief can not use the transmitter because the system and method will never verify the user to permit the use of the rolling code for access.

Support For The Claims

For support for combining and separating the codes, please see page 15, lines 13 to 25 and Fig 5 (shows transmitter) and for action of the receiver, see page 18 at line 10 and Fig 4 as well as Fig 8, see mention of Fig 8 at page 18 line 2.

For support for not transmitting back from the receiver to the transmitter, please see Figures 4 and 8 and pages 10 and 18 where the figures do not show the receiver transmitting back to the transmitter.

For support for using an algorithm as described and claimed, please see USP 5,949,349 to Farris at Col 1 lines 29 to 33 and especially at Col. 4, line 65 to Col. 5, line 4. The '349 patent is incorporated by reference at several places in the instant specification, see page 7, line 7, page 8, line 32, page 10, line 27 etc.

The Commissioner is hereby authorized to charge any additional fees which may be required with respect to this communication, or credit any overpayment, to Deposit Account No. 06-1135.

Respectfully submitted,

FITCH, EVEN, TABIN & FLANNERY

Dated: May 6, 2009

Timothy E. Levstik
Registration No. 30,192

120 South LaSalle Street, Suite 1600
Chicago, Illinois 60603-3406
Telephone (312) 577-7000
Facsimile (312) 577-7007
533876